



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/719,428	11/21/2003	Vincent J. Zimmer	INTEL/17852	3414
34431 7590 07/16/2007 HANLEY, FLIGHT & ZIMMERMAN, LLC 150 S. WACKER DRIVE SUITE 2100 CHICAGO, IL 60606			EXAMINER SHIFERAW, ELENI A	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 07/16/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	Application No. 10/719,428	Applicant(s) ZIMMER ET AL.	
	Examiner Eleni A. Shiferaw	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 21 November 2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 21 November 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>04/06/2004 and 08/16/2006</u> . | 6) <input type="checkbox"/> Other: _____  |

***DETAILED ACTION***

***Claims Status***

1. Claims 1-32 are presented for examination and pending.

***Information Disclosure Statement***

2. The Information disclosure statement (IDS) submitted on 04/06/2004 and 08/16/2006 are considered and an initialized and dated copy of Applicant's IDS form 1449 is attached to this Office action.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

- 3.1 Claims 1-7, 9-17, 19-27, and 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Compaq Computer Corporation, Hewlett-Packard Company, IBM Corporation, Intel corporation and Microsoft Corporation, published on September 9, 2001, herein after (CHIIM) in view of Kuznetsov et al. USPN 5,483,649.

As per claim 1, CHIIM discloses a method comprising:

Art Unit: 2136

generating at least one descriptor (figure 7-1; *descriptors of RSDT table, FACP table, DSDT table, ACPI, e.g. FIRM*) in a pre-boot environment (section 7.2 line 5; *pre-boot entities including ACPI*);

storing the at least one descriptor (figure 7-1; *descriptors of RSDT table, FACP table, DSDT table, ACPI*) in a resource protection list (*RSDT table, FACP table, DSDT table, ACPI of fig. 7-1*); and

storing the resource protection list in a location accessible in a post-boot environment (sections 7.2 and 7.1; *storage of data/code using ACPI in a pre-boot and post-boot OS is reading these data*).

CHIIM discloses an ACPI table usage and post-boot OS accessing/reading data of ACPI that is stored in a pre-boot environment and instantiation of event log array structures comprising hash within validation certificate for validation (see sections 7.2, and 7.2.1-7.2.2.2.3), CHIM also discloses a security properties of a platform protection profile (section 1.3.1), and PCR register usage that define PCR assignments used for boot time integrity metrics and methodology for collecting the metrics (section 2.2). CHIIM fails to explicitly disclose a descriptor in a pre-boot environment being associated with establishing a protection policy for at least one firmware resource. Kuznetsov et al. discloses a computer security system comprising defined software access privilege (col. 16 lines 39-41; descriptor) in a passive operating mode (col. 17 lines 25-29; pre-boot) that is associated with access rights, comprising software privilege of changing files and privilege of writing, (col. 17 lines 10-19; software protection policy) using protection program support module (fig. 8 element 120B).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Kuznetsov et al. within the system of CHIIM because they are analogous in platform protection. One would have been motivated to incorporate the teachings of establishing a protection policy for a firmware by generating a descriptor in a pre-boot environment because it would authenticate software access to provide or deny access to protected resources based on software privileges, before/after operating system is executed.

Regarding claim 11, it recites an apparatus claim and has similar limitations as claim 1, and it is being rejected based on the same rational as claim 1. In addition, CHIIM teaches the additional limitations of claim 11 wherein

- a processor system (6.2.3 and fig. 1-1; *OS processor*); and
- a memory communicatively coupled to the processor system, the memory including stored instructions that enable the processor system to perform the method claim 1 (6.3.2.5, fig. 1-1, and 7.1; *hard disk memory*).

Regarding claim 21, it recites a computer readable medium claim and has similar limitations as claim 1, and it is being rejected based on the same rational as claim 1.

Regarding claim 31, it recites an apparatus claim and has similar limitations as claim 1, and it is being rejected based on the same rational as claim 1. In addition, CHIIM teaches the additional limitations of claim 31 wherein

Art Unit: 2136

a processor system (6.2.3 and fig. 1-1; *OS processor*); and  
a flash memory communicatively coupled to the processor system, the flash memory including stored instructions that enable the processor system to perform the method of claim 1 (6.3.2.5, fig. 1-1, 3.1, and 2.2.3; *ROM*).

As per claims 2, 12 and 22, CHIIM further teaches a method/apparatus/medium further comprising initializing the at least one firmware resource in the pre-boot environment (page 25 section 6.1).

As per claims 3, 13, and 24, CHIIM further discloses a method/apparatus/medium further comprising generating at least one hash code based on the at least one descriptor (7.2, 6.1, 6.2.3, and 6.3.2.1; *code hashing storing in ACPI*)

Regarding claims 4, 14, and 25, CHIIM discloses a method/apparatus/medium further comprising storing the at least one hash code in a trusted protection module platform configuration register (7.2 and 6.3.2.1; *TCG\_HashLogExtendEvent hash code stored within ACPI data area that is defined in fig. 7-1*).

Regarding claims 5, 15, and 26, CHIIM discloses a method/apparatus/medium further comprising storing the at least one descriptor in an advanced configuration and power interface differentiated system descriptor table (6.3 and figure 7-1; *ACPI*).

Art Unit: 2136

As per claims 6, 16, 23, and 32, CHIIM discloses a method/apparatus/medium wherein the at least one firmware resource includes at least one of a register region, a firmware data memory region, a firmware code memory region, and a hand-off information memory region (6.2.3; *handoff code*).

As per claim 7, CHIIM discloses a method/apparatus/medium wherein the pre-boot environment comprises executing at least one of a basic input output system and an extensible firmware interface (sections 6.1-6.2.2; *BIOS and extending code interface execution*).

Regarding claims 9, 20, and 30, CHIIM teaches a method/apparatus/medium, further comprising establishing a resource protection policy in the post-boot environment based on the resource protection list (CHIIM section 7.2).

Regarding claims 10, 19, and 29, CHIIM discloses a method/apparatus/medium, further comprising enabling the resource protection list to be validated in the post-boot environment (section 7.2-7.2.2.2.3).

As per claims 17 and 27, CHIIM discloses an apparatus wherein the instructions stored in the memory enable the processor system to execute at least one of a basic input output system and an extensible firmware interface in the pre-boot environment (sections 6.1-6.2.2; *BIOS and extending code interface execution in a pre boot*).

Art Unit: 2136

3.2 Claims 8, 18, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Compaq Computer Corporation, Hewlett-Packard Company, IBM Corporation, Intel corporation and Microsoft Corporation, published on September 9, 2001, herein after (CHIIM) and Kuznetsov et al. USPN 5,483,649, and further in view of McDonnal et al. USPN 5,796,825.

As per claims 8, 18, and 28, CHIIM and Kuznetsov et al. teach all the subject matter as described above. In addition, CHIIM and Kuznetsov et al. disclose a method wherein storing the resource protection list comprises storing the resource protection list in a location accessible by an operating system in the post-boot environment (CHIIM section 7.2, and Kuznetsov et al. col. 15 lines 30-64). CHIIM and Kuznetsov et al. fail to teach a method wherein storing the resource protection list comprises storing the resource protection list in a location accessible by at least one of a secure virtual machine monitor (VMM) and/or in the post-boot environment. However McDonnal et al. teaches a VMM with privileged space memory (fig. 1 element 140), boot control file (fig. 1 element 152) that stores protected/encrypted files and unprotected files (fig. 1 elements 153, and 160) for boot access protection and VMM of win32-compliant executing/accessing encrypted/protected files (col. 13 lines 63-col. 14 lines 15), after the loading of OS kernel (col. 13 lines 6-7, and col. 12 lines 42-col. 14 lines 15).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of VMM within the combination system of CHIIM and Kuznetsov et al. because they are analogous in boot access protection. One would have been motivated to do so because it would use secure virtual machine monitor to access



Art Unit: 2136

protection list/boot control file and protect a resource.

*Conclusion*

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867.

The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



June 20, 2007

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
7,907